(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 December 2002 (05.12.2002)

PCT

(10) International Publication Number
WO 02/098042 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US02/15201

(22) International Filing Date: 15 May 2002 (15.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/867,747 31 May 2001 (31.05.2001) US

(71) Applicant: CONTENTGUARD HOLDINGS, INC. [US/US]; Suite 200-M, 103 Foulk Road, Wilmington, DE 19803 (US).

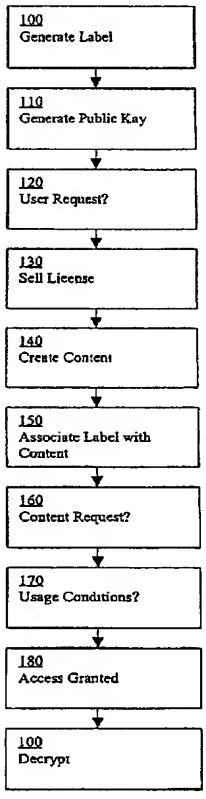
(72) Inventors: TADAYON, Bijan; 20920 Scottsbury Dr., Germantown, MD 20876 (US). NAHIDIPOUR, Aram; 3224 145th Place, SE, Mill Creek, WA 98012 (US). WANG, Xin; 3005 Shrine Place, #8, Los Angeles, CA 90007 (US). RALEY, Michael, C.; 12834 Verdura Avenue, Downey, CA 90242 (US). LAO, Guillermo; 5531 Lorna Street, Torrance, CA 90503 (US). TA, Thanh, T.; 18694 Stratton Lane, Huntington Beach, CA 92648 (US).

(74) Agent: KAUFMAN, Marc, S.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR ESTABLISHING USAGE RIGHTS FOR DIGITAL CONTENT TO BE CREATED IN THE FUTURE



(57) Abstract: Usage rights for a digital work are established prior to creation of the corresponding content. The rights can be associated with the content after the content is created. A content creation, such as a video recorder or a still camera, device can store labels of the rights and can associate usage rights with content in real time as the content is created.

WO 02/098042 A2

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR ESTABLISHING USAGE RIGHTS FOR DIGITAL CONTENT TO BE CREATED IN THE FUTURE

BACKGROUND OF THE INVENTION

[0001] This invention relates generally to assignment of usage rights for digital works. In particular, this invention relates to establishing usage rights for before the content is created.

[0002] One of the most important issues impeding the widespread distribution of digital works via electronic means, and the Internet in particular, is the current lack of protection of intellectual property rights of content owners during the distribution and the usage of the digital content. Efforts to resolve these issues have been termed "Intellectual Property Rights Management" ("IPRM"), "Digital Property Rights Management" ("DPRM"), "Intellectual Property Management" ("IPM"), "Rights Management" ("RM"), and "Electronic Copyright Management" ("ECM"), collectively referred to as "Digital Rights Management" ("DRM") herein.

[0003] Due to the expansion of the Internet in the recent years, and the issues relating to privacy, authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, document protection, and collection of licensing fees DRM has become even more important. Because the Internet is such a widely used network whereby many computer users communicate and trade ideas and information, the freedom at which electronically published works are reproduced and distributed is widespread and commonplace.

[0004] Two basic types DRM of schemes have been employed to attempt to solve the document protection problem: secure containers and trusted systems. A "secure container" (or simply an encrypted document) offers a way to keep document contents encrypted until a set of authorization

conditions are met and some copyright terms are honored (e.g., payment for use). After the various conditions and terms are verified with the document provider, the document is released to the user in clear form. Commercial products such as IBM's CRYPTOLOPES™ and InterTrust's DIGIBOXES™ fall into this category. Clearly, the secure container approach provides a solution to protecting the document during delivery over insecure channels, but does not provide any mechanism to prevent legitimate users from obtaining the clear document and then using and redistributing it in violation of content owners' intellectual property.

[0005] Cryptographic mechanisms are typically used to encrypt (or "encipher") documents that are then distributed and stored publicly, and ultimately privately deciphered by authorized users. This provides a basic form of protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium.

[0006] In the "trusted system" approach, the entire system is responsible for preventing unauthorized use and distribution of the document. Building a trusted system usually entails introducing new hardware such as a secure processor, secure storage and secure rendering devices. This also requires that all software applications that run on trusted systems be certified to be trusted. While building tamper-proof trusted systems is a real challenge to existing technologies, current market trends suggest that open and untrusted systems such as PC and workstations using browsers to access the Web, will be the dominant systems used to access digital works. In this sense, existing computing environments such as PCs and workstations equipped with popular operating systems (e.g., Windows™, Linux™, and UNIX) and rendering applications such as browsers are not trusted systems and cannot be made trusted without significantly altering their architectures. Of course,

alteration of the architecture defeats a primary purpose of the Web, i.e. flexibility and compatibility.

[0007] U.S. Patent Numbers 5,530,235, 5,634,012;, 5,715,403, 5,638,443, and 5,629,980 introduced many basic concept of DRM. All of these patents are hereby incorporated herein by reference in their entirety. U.S. patent 5,634,012 discloses a system for controlling the distribution of digital documents. Each rendering device has a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for carrying out usage rights associated with a document. Usage rights are encapsulated with the content or otherwise associated with the digital work to travel with the content. The usage rights can permit various types of use such as, viewing only, use once, distribution, and the like. Rights can be granted based on payment or other conditions.

[0008] In conventional DRM techniques, a content owner, or other authorized party, specifies the rights after the content has been created and protects, e.g. encrypts, the content at the same time. A private key is used to encrypt the content, and a label is generated which specifies the usage rights. The rights label and the protected content are then associated and stored. A license to the content can later be generated for a user to permit the user to use or access the content. The license includes a private key which has been encrypted using a public key in known manner.

[0009] To access the content, the private key can be used to decrypt the encrypted public key, allowing the user to decrypt the content. This technique works well if the content is available at the time of the rights specification. However, this technique breaks-down if one wants to specify rights for content and issue a license for the content before the content is available. For example, a distributor of streaming video to a live future event, or of photographs to a future event, may want to begin selling licenses to the content prior to the event. Conventional DRM systems fall short of presenting

processes for improving the security, user interface, organization, structure, and accuracy of the DRM system, particularly for those works that are not yet in existence.

SUMMARY OF THE INVENTION

[0010] An object of the invention is to obviate the problems noted above in the prior technology and permit usage rights to be assigned to a work prior to creation of the work.

[0011] A first aspect of the invention is a method for creating a digital work having content and usage rights related to the content. The method comprises generating a label having usage rights associated with content of a digital work before the content is created, associating the label with the content after the content is created, and securing the content and the label.

[0012] A second aspect of the invention is a system for providing usage rights for a digital work. The system comprises a content creation device for creating a digital content, a rights assignment engine associated with the content creation device, the rights assignment engine automatically attaching predetermined usage rights to the created digital content, and an identification device for identifying an authorized user and allowing the authorized user to gain access to the digital content in accordance with the usage rights.

[0013] A third aspect of the invention is a method for creating a digital work having content and usage rights related to the content. The method comprises generating a label having usage rights associated with content of a digital work before the content is created, storing the label in a content creation device, creating content with the content creation device, associating the label with the content after the content is created, and securing the content and the label.

BRIEF DESCRIPTION OF THE DRAWING

[0014] Various embodiments of this invention will be described in detail, with reference to the following figures, wherein:

[0015] Fig. 1 is a flowchart of a method for providing usage rights for digital content before creation of the content in accordance with the an embodiment of the invention; and

[0016] Fig. 2 is a content creation device for providing usage rights for digital content to be created in the future in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0017] The phrase "digital work" as used herein refers to any type of element having content in computed readable form. "Content" as used herein refers to the viewable or otherwise usable portion of a digital work. The phrase "usage rights" refers to permissions granted to a user of an existing digital work or a digital work to be created in the future with respect to use, access, distribution, and the like of the content of the work. In addition, usage rights may have one or more conditions which must be satisfied before the permissions may be exercised.

[0018] Fig. 1 illustrates an embodiment of a method for providing usage rights for content of a digital work before the content is created. In step 100 a label specifying usage rights, to be associated with digital content that is not yet created, is generated. The usage rights label can include usage rights, such as the right to print, copy, alter, edit or view the digital work or any other right, permission, or restriction, such as those contained in the XrML™ language or other usage rights grammar. Alternatively, the usage rights label may include merely an identification of the work and other descriptive data and the specific granted usage rights can be contained in the license

discussed below. In the case of using the XrML™ language, the label can be an extensible markup language (XML) document specifying the usage rights. In addition, the future content can have many different versions of usage rights and thus a label can be generated for each version. In step 110, a key, such as a conventional public key, is generated in a known manner and associated with the label.

[0019] In step 120, a user request for use of, i.e. a license to, the content to be created is received. Keep in mind that the content itself need not be in existence yet. For example, the content can be a video recording or stream of a sporting event to occur in the future. In step 130, a distributor of the content, or another authorized party, issues a license to the user. The license can include a private key corresponding to the public key generated in step 110 and may include usage rights or other descriptive data. Once, again, keep in mind that the content itself need not be in existence yet. Accordingly, the distributor is able to sell a license to view the event prior to the event.

[0020] In step 140, the content is created. Of course, this step can be accomplished by another party. However the content is created, the salient point is that the content somehow comes into existence after rights are assigned for it. After the content is created, the usage rights label is associated with the content in step 150. The usage rights label can be encapsulated with or attached to the content whereby copies of the digital work will also carry the usage rights label. Alternatively, the label can be stored separately from the content but be associated through flags, calls, or the like. Therefore, the term "associated" as used herein refers broadly to creating a correspondence between the content and the label so the label will be applied to the content. Once the usage rights label is associated with the content, the content is secured using the key generated in step 110. The digital content can be secured through any form of encryption or other known

technique. For example pretty good privacy (PGP) encryption procedures can be used.

[0021] In step 160, the process determines whether there is a request for access to the secured digital content. If there are no requests, the process waits for a request. However, if there is a request for access, the process proceeds to step 170 where the usage rights associated with the digital work and/or license are checked to determine whether all the conditions, such as payment, associated with the usage rights have been satisfied. If all the conditions have been satisfied, the process proceeds to step 180 in which access to the content is granted, i.e., the content is downloaded, streamed, or otherwise transferred to the user. In step 190, the user's private key is used to decrypt the content in a known manner.

[0022] The association of the usage rights with the content may occur in a variety of ways. For example, if the usage rights will be the same for the entire content of a digital work, the usage rights can be attached when the digital work is processed for deposit in a distribution server of other device. However, if the content of the digital work has a variety of different usage rights for various components, the usage rights can be attached as the work is being created. Various authoring tools and/or digital work assembling tools can be utilized for providing an automated process of attaching the usage rights. Because each part of a digital work can have its own usage rights, there can be instances where the usage rights of a "part" will be different from its parent. As such, conflict rules can be established to dictate when and how a right may be exercised.

[0023] Fig. 2 illustrates a content creation device, a video recorder, in accordance with a preferred embodiment of the invention. The content creation device 300 includes a controller 302, a LCD display 304, a smart-card reader 306, a memory 307, a keypad 308, a rights assignment engine 310, eye/iris recognition sensors 312, a cable connection 313, a handle 314,

and symmetric finger print recognition sensors 316,318. Also, lens system 320 permits recording of video images. Controller 302 and rights assignment engine 310 of the preferred embodiment are accomplished through a microprocessor based device programmed in a desired manner.

[0024] While Fig. 3 shows the controller 302 and the rights assignment engine 310 as separate units, the functions performed by these units may be combined in one processor or may be further divided among plural processors such as digital signal processors and/or performed by dedicated hardware such as application specific integrated circuits (ASIC), e.g., hard-wired electronic or logic circuits or programmable logic devices., or other hardware or software implementations.

[0025] The smart-card reader 306 can be used for reading cards inserted therein. For example, a license, usage rights, or identification can be embedded in the card and communicated to the controller 302 and/or the rights assignment engine 310. LCD display 304, the smart card reader 306, keypad 308 and software interfaces constitute a user interface of creation server 300. The user interface permits a user to input information such as identification data, and access requests and provides feedback as to operation of creation device 300. The content creation device 300 of the preferred embodiment is a video recorder, however, it can be any type of recording device, for example, a still-image camera, an animation generator, or an audio recorder.

[0026] The rights assignment engine 310 can be accessed via the cable connection 313. For example, a rights assignment computer (not illustrated), such as any computer running XrML™ and related tools, can be coupled to the rights assignment engine 310 via cable connection 313 to download a usage rights label or template, similar to the label described above, indicating usage rights for content to be created by the content creation device 300 in the future. Any content created by the content creation device 300 will

automatically be associated with the usage rights label or labels stored in rights assignment engine 310. Alternatively, the usage rights label can be composed using the user interface of creation device 300. In either case, one or more labels are and corresponding keys generated and stored in rights assignment engine 310 along with instructions indicating how the labels are to be assigned to content recorded by creation device. 300.

[0027] The instructions can cause the usage rights labels to be assigned in any manner and can include any permissions and/or restrictions. For example, in the case of a video recorder, each part of the video sequence or frames can selectively be assigned different rights. This makes the rights assignment process very flexible and dynamic and permits rights assignment to be made in real time as content is created or prior to creation.

[0028] The content creation device 300 can utilize a unique device ID, a user's smart card, PKI technology, a PIN, or any biometrics system to assign rights based on the identity of the user, the recording device itself, the data on the smart card, or the like. For example, fingerprint recognition sensors 316, 318 or iris recognition sensor 312 can be used for recognition or authentication of the user's identify to permit rights assignment engine 310 to use a corresponding set of rights associated with the user. For example, all content recorded by person A will have one set of rights and all content recorded by person B will have a different set of rights.

[0029] The content creation device 300 records content in a conventional manner. However, labels and keys generated in steps 100 and 110 described above are stored and associated with content recorded by content recorder 300 during or soon after recording. Accordingly, steps 140 and 150 described above are also accomplished by content creation device 300. For security purposes, a token or pre-paid card (or magnetic card and smart card, or any of its variations, such as memory-type or synchronous communication card, ISO 7816-compliant card, EMV-type card) can be used for the storage

of fees and micro-payments, or keeping track of those fees with associated rights. Such cards can be read using the smart card reader 306.

[0030] It can be seen that the invention permits usage rights for a work to be created and associated with content prior to the creation of the content. The usage rights define how the future digital work may be used and distributed. These pre-established usage rights become apart of the future digital work and controls the usage and distribution of the content of such work.

[0031] In the preferred embodiment, after the rights have been established for a future content, a private key associated with the future content is assigned and a rights label is generated. This private key, along with the rights label, is stored. A user can purchase the content (present or future) after the label has been inserted into the main server. After the content is purchased, the content owner can get a license for encryption which contains the public key encrypted by a private key. Alternatively, a single symmetric key can be used.

[0032] The invention can be used in a subscription model (for example, for magazine or marketing reports) in which the future issues of the content have not been published, but the rights for those issues have already been assigned and stored. At an appropriate future time, the rights will be associated with the corresponding content. For example, by selling the content of a future event on a web site before the actual event, the traffic of the Web site can be drastically reduced and distributed over a longer period of time, making the requirements for the servers and the Web site easier to satisfy and less expensive to operate. Note, however, that the Web site selling the rights or tickets, i.e. the license, might be different from the Web site providing the content later on.

[0033] Also, the invention allows a newspaper editor, for example, to send a camera crew to record content without worrying about the pictures being compromised in any way (for example, altered, edited, viewed by unauthorized personnel, or hidden and separately sold to another newspaper organization). In fact, the camera crew may have no rights whatsoever in the content as soon as the content is recorded.

[0034] Alternatively the editor can set the rights in such a way that the first 10 pictures, for example, will belong to the newspaper (work-related), and the next five pictures will belong to the cameraman (for personal use). This example illustrates the flexibility, security, confidence, certainty, and multiple relationships that can be arranged between parties (the cameraman and the editor in this example).

[0035] All future content may be assigned a content ID prior to existence of the content. Given the content ID information and the license for encryption, the content can be encrypted after creation in a manner that is available to be used by the users who have purchased the license. However, if the content ID information and the license for encryption are not available, access to the content shall be denied.

[0036] Further, a predetermined symmetric key can be generated in advance of content creation, and stored with the rights label. Afterwards, the same key can be used to encrypt the content once it is created. However, as noted above every user can receive a different key. In another alternative, the user can be given an authorization token, which the user can exchange for the license later on.

[0037] The controller 302 can process the security parameters and the rights management steps. Lost-card verification, lost-card reports, card-usage reports, security alert reports, and tracking reports can be associated

or combined with the rights management reports, such as reports for revoked rights, denied rights, renewed rights, usage patterns, and micro-payments.

[0038] The invention may be readily implemented in software using object or object-oriented software development environment that provides portable source code that can be used on a variety of computer hardware platforms. For example the software can be written in the JAVA™ language and run in a JAVA™ virtual machine. Alternatively, the disclosed operations may be implemented partially or fully in a hardware using standard logic circuits or VLSI designs. The hardware can include any type of general purpose computer, dedicated computer, or other devices.

[0039] The distribution, accounting, and other functions of the distributor and clearinghouse can be accomplished by any party on any device. For example, the content can be rendered on an ebook reader or PDA in response to entry of a code or insertion of a smartcard into a reader and accounting can be accomplished when the digital work or accounting data is returned to a specific source. The division of tasks disclosed herein is only an example. Usage rights and or accounting data can be encapsulated with the digital work or can be stored separately. Code for rendering, decrypting, or otherwise permitting or limiting use of the content can be stored on any device or can be encapsulated with the digital work. Any distribution arrangement can be used with the invention and such arrangements can include any combination of devices, such as personal computers, servers, PDAs, and the like communicating with one another in any manner as is necessary to transfer the desired information.

[0040] The invention has been described in connection with the above embodiments. However, it should be appreciated that many alternates, modifications and variations may be made to the embodiments of the invention without departing from the scope of the invention as defined by the appended claims and legal equivalents.

What is Claimed is:

1. A method for creating a digital work having content and usage rights related to the content, the method comprising:

generating a label having usage rights associated with content of a digital work before the content is created;

associating the label with the content after the content is created and;

securing the content and the label.

2. The method of claim 1, wherein said securing step comprises encrypting and storing the content and the label.

3. The method of claim 1, further comprising granting access to the content in accordance with the usage rights.

4. The method of claim 1, wherein said generating step comprises generating usage rights specifying a user's right to at least one of alter, edit, copy, print, or view the content.

5. The method of claim 1, further comprising the step of creating at least one of a written, aural, graphical, audio, pictorial or video based element as the content after said generating step and before said associating step.

6. The method of claim 1, wherein said generating step further comprises:

assigning a predetermined secure key to be associated with the content and wherein said securing step comprises encrypting the content and the label with the secure key.

7. A method of claim 5, wherein said creating step comprises recording content with a recording device and wherein said associating step and said securing step are accomplished by the recording device.

8 A method as recited in claim 7, wherein said generating step comprises creating the label in an external computing device and downloading the label into the recording device prior to said associating step.

9. A method as recited in claim 7, wherein said generating step comprises creating the label in the recording device prior to said associating step.

10. A system for creating a digital work having content and usage rights, the system comprising:

a content creation device for creating a digital content;

a rights assignment engine associated with the content creative device, the rights assignment engine automatically attaching predetermined usage rights to the content and securing the content with the usage rights.

11. A system as recited in claim 10, further comprising:

an identification device for identifying user of the content creation device; and,

means for determining the usage rights based on the user.

12. The system of claim 10 wherein said content creation device comprises one of a still-image camera, an audio recorder, or a video recorder.

13. The system of claim 11, wherein the identification device comprises, a biometrics sensor

14. The system of claim 11, further comprising a secure storage medium for the storage of fee and payment information associated with the usage rights.

15. The system of claim 11, wherein said content creation device comprises a video recorder.

16. The system of claim 11, wherein said content creation device comprises a still picture camera.

17. A method for creating a digital work having content and usage rights related to the content, the method comprising:

generating a label having usage rights associated to be associated with content of a digital work before the content is created;

storing the label in a content creation device device;

creating the content with the content creation device;

associating the label with the content after the content is created and;

securing the content and the label.

18. The method of claim 17, wherein said securing step comprises encrypting and storing the content and the label.

19. The method of claim 17, further comprising granting access to the content in accordance with the usage rights.

20. The method of claim 17, wherein said generating step comprises generating usage rights specifying a user's right to at least one of alter, edit, copy, print, or view the content.

21. The method of claim 17, wherein said creating step comprises creating at least one of a written, aural, graphical, audio, pictorial or video based element as the content.

22. The method of claim 17, wherein said generating step further comprises:

assigning a predetermined secure key to be associated with the content and wherein said securing step comprises encrypting the content and the label with the secure key.

23. A method of claim 22 wherein said creating step comprises making a recording with a recording device and wherein said associating step and said securing step are accomplished by the recording device.

24. A method as recited in claim 23, wherein said generating step comprises creating the label in a computing device and downloading the label into the recording device prior to said associating step.

25. A method as recited in claim 23, wherein said generating step comprises creating the label in the recording device prior to said associating step.

Fig. 1

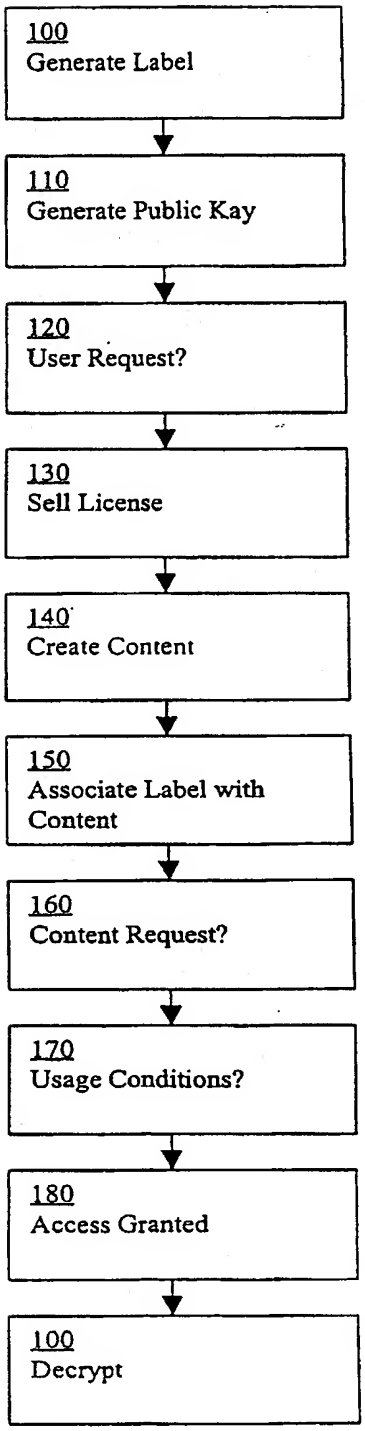


FIG. 2